Are Mobile Payments Safe?

Talk About Payments Webinar

October 5, 2017

Dave Lott

Payments Risk Expert

Federal Reserve Bank of Atlanta

Connection Information

- Webinar Link: https://www.webcaster4.com/Webcast/Page/577/22159
- Choose to listen with your PC speakers.
  - If you are having trouble hearing through your speakers
    - Call-in Number: 1-888-625-5230
    - Participant Code: 7183 1584#
- Ask a Question:
  - Click the “Ask Question” button in the webinar tool
  - Email rapid@stls.frb.org

Retail Payments Risk Forum

- We serve as a catalyst for collaboration in the consumer and commercial payments risk management arena. We:
  - Conduct research and provide analysis
  - Convene and share with interested parties
  - Promote actions to mitigate risk

Take On Payments weekly blog

- http://takeonpayments.frbatlanta.org

Retail Payments Risk Forum webpage

- https://www.frbatlanta.org/rprf

Mobile Payments Industry Workgroup (MPIW)

- Collaborative effort of 40+ mobile payment industry experts
- Share perspectives on mobile topics of common concern, e.g., consumer adoption, security, tokenization, nonbank solutions, regulation
- Form subgroups to explore key issues
- Publish whitepapers and briefs for broader industry education

  - Large/small FIs, credit unions
  - Card networks
  - Merchants
  - Payment processors
  - Clearing/settlement orgs
  - Non-bank technology providers
  - Mobile network operators
  - Handset & chip manufacturers
  - Mobile solution providers
  - Industry trade associations (CTIA, Conexxus, MAG, NACHA, Secure Technology Alliance)

Agenda

- Current Mobile Landscape
- Mobile Benefits & Risks
- Consumer Security Behaviors
- Mobile Security Best Practices
- Questions & Discussion

Mobile As Key Driver in Payments?

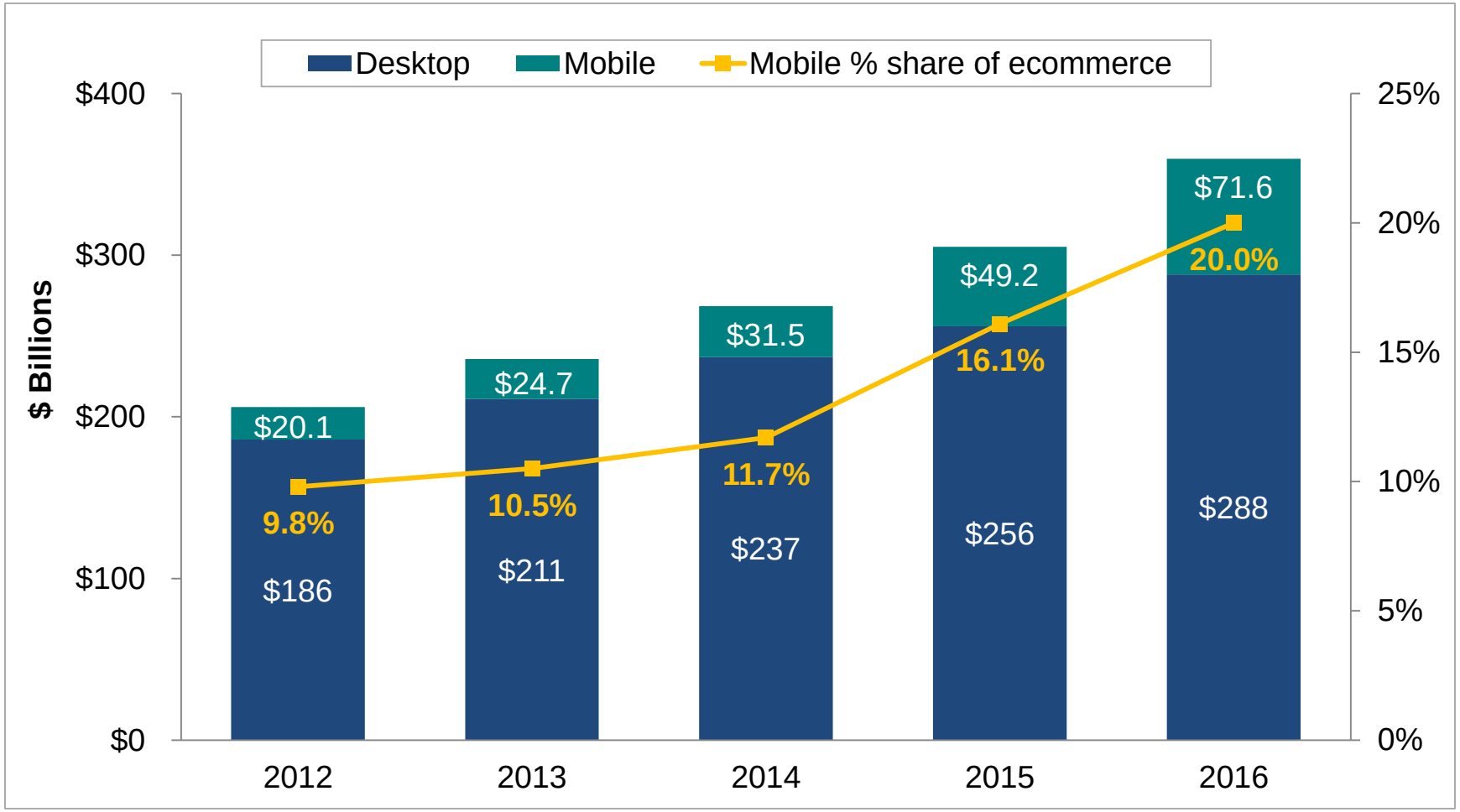
Joseph Van Os / Getty Images

Who doesn't have a smartphone?

- 87% of U.S. adults have a mobile phone
- 77% of U.S. adults own a smartphone

Source: 2016 Consumers and Financial Services, Board of Governors of the Federal Reserve System

Mobile Payments Driving Increase in eCommerce/CNP Volume



Source: comScore, 2017

Mobile Wallet Ecosystem

2006-2008

Remote Payments - SMS & Internet

- PayPal *Text to Buy*
- *Text Buy It*

Mobile App Stores

- Apple
- Android

Contactless Cards

- Visa payWave
- MasterCard paypass

Direct Carrier Billing

2009-2010

Mobile Browser

mPOS

- Square

Proliferation of Mobile Apps

2011

QR Codes

- LevelUp

NFC + SE Mobile Wallet

- Google wallet

Mobile Prepaid

- American Express serve

2012

mPOS

- PayPal HERE

NFC Wallet

- Soft Card

Digital Wallet

- Google wallet
- Apple Passbook
- PayPal
- V.me by Visa

Prepaid Account

- Bluebird

Mobile Bank Account

- GoBank

2013-2014

NFC + HCE

- Google wallet

Beacon BLE

- PayPal

NFC + token

- Apple Pay

Digital Wallet

- VISA Checkout
- MasterPass

2015-2016

Merchant Apps

- Currentc
- Walmart Pay

FI Wallet

- Capital One Pay
- CUWallet

NFC + HCE

- pay

Virtual Swipe

- Samsung pay

Digital Wallet

- AMEX Express Checkout

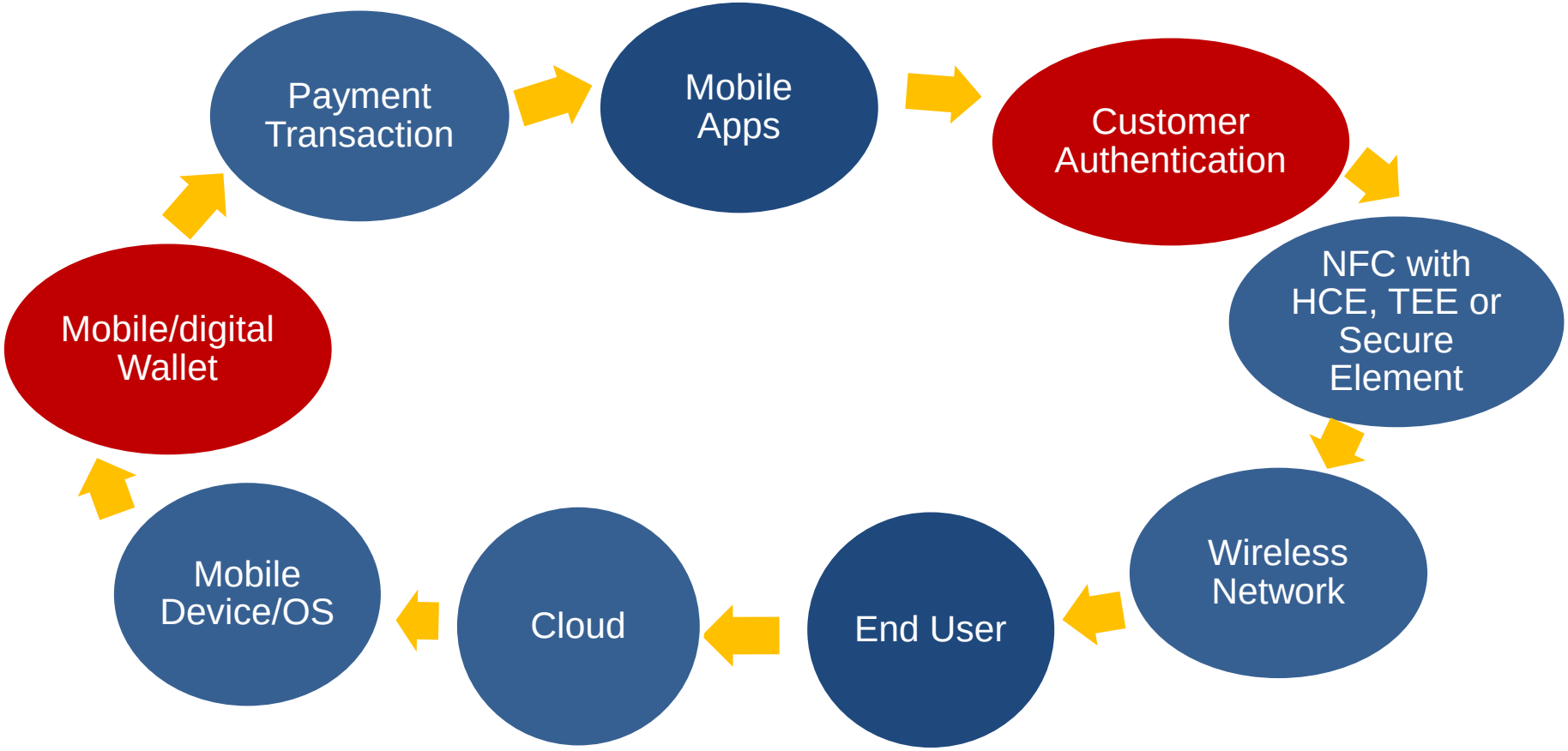
Mobile Payment Opportunities

- Many advantages with mobile payments
  - More security elements – geo-location, biometrics
  - Merchant efficiencies
  - Consumer convenience, demographic & life style changes
  - Marketing & location-based services
  - Convergence with value-added services
  - Financial inclusion – consumer and merchant
    - Highly successful in developing countries
    - Reloadable prepaid cards primary product used to date
- Primary reasons given by merchants to support mobile payments
  - 85% customer convenience
  - 61% meet customer's expectations

Mobile Payments Environment is Changing Rapidly

- New technologies and payment models
- Growing influence of non-banks
- Channel convergence across POS, mobile and digital
  - Poses more complex payment security risks
  - Creates more payment security gaps
  - Sophisticated and increasing fraud threats across channels, particularly to online
  - Driving need for multi-layered security approach
- Faster “near real-time” payments are a reality and may create new opportunities for mobile

Multiple Risk Points Must Be Managed

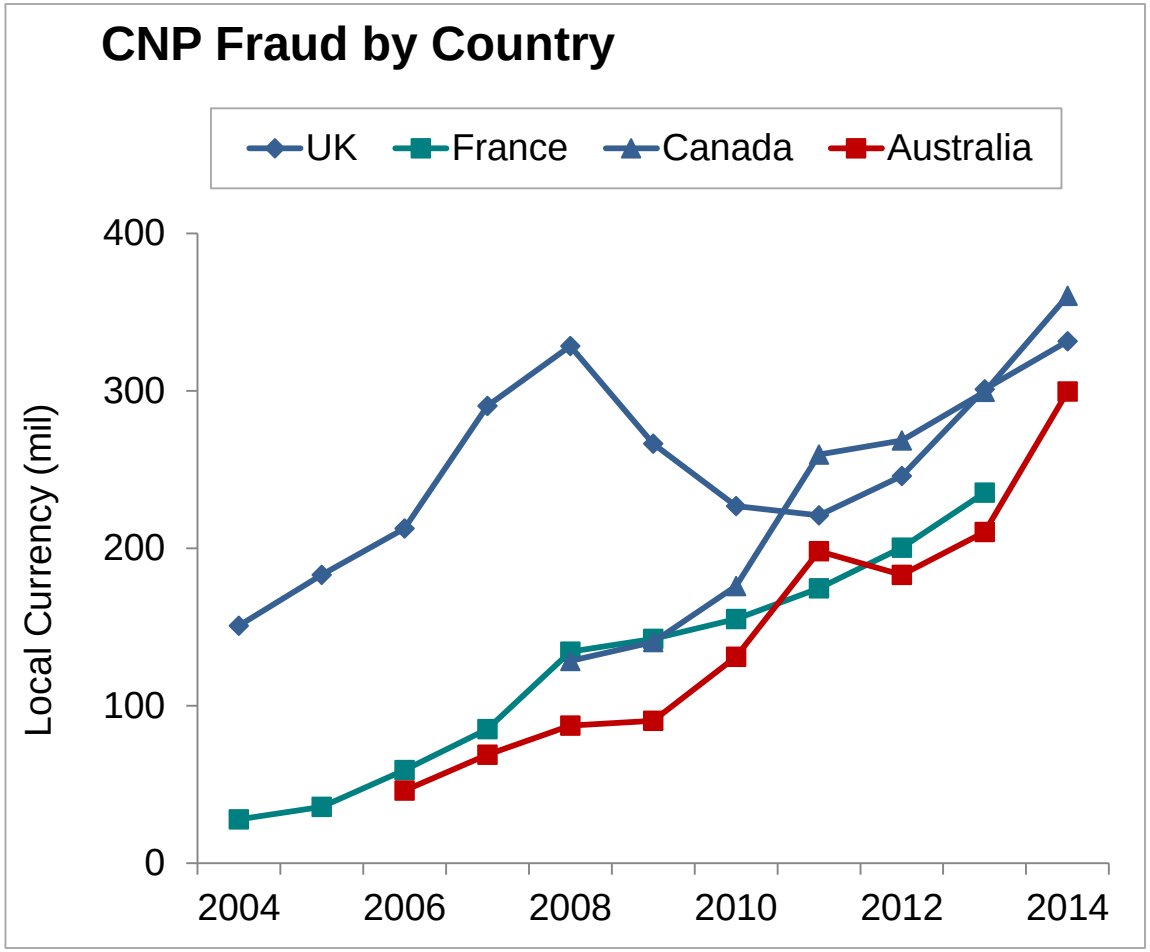


Mobile/Digital Wallet Expansion to eCommerce Increases Security Challenges

Mobile/digital wallets	Technologies	Acceptance channels	Examples
'Pay' wallets	NFC + eSE	In-store, in-app, online	Apple Pay
	NFC + HCE	In-store, in-app, online	pay
	NFC + TEE / MST	In-store, in-app	SAMSUNG pay
Merchant-centric	Cloud + QR code	In-store	Walmart Pay
Payment service providers	Cloud	In-store, in-app, online	PayPal
		In-app, online	amazon pay
FI-centric Wallets	Cloud + QR code	In-store, in-app, online	Pay
	NFC + HCE	In-store	WF, Capital One
Digital Wallets	Cloud	In-app, online	AMEX EXPRESS CHECKOUT, VISA Checkout, masterpass
	NFC + HCE	In-store	

Source: Payment Strategies, Federal Reserve Bank of Boston, 2017

EMV Card Migration Does NOT Address CNP Fraud – Only Makes It Worse



- Criminal uses stolen payment card credentials to pay for purchase online, via call center, mobile device or mail order
  - 25% of total global fraud losses in 2015 (~ $4B) (Nilson Report)
  - 45% of total U.S. card fraud (RSA, 2015)

Source: Retail Payments Risk Forum, Federal Reserve Bank of Atlanta, 2015

Mobile Payments Fraud

- 2016 Lexis Nexis Cost of Fraud study results:
  - Fraud losses are 1.47% of sales volume
  - Places value of mobile fraud at 3 times the initial loss amount
  - Mobile transactions represent 14% of overall merchant transactions, but fraudulent mobile transactions represent 21% of the merchant's fraudulent transactions
  - Large remote m-commerce merchants use an average of 5 – 6 fraud mitigation solutions
    - Primary tools employed:
      - Transaction verification services
      - Geolocation
      - Browser/malware tracking

MPIW Identified Need to Assess Mobile/Digital Fraud

- Considered potential risks and security gaps related to in-store and remote mobile payments
- Conducted comparative analysis of four mobile/CNP wallet models
  1. "Pay" wallets - Apple Pay, Android Pay, Samsung Pay
     - Use NFC, EMV ID&V for POS and mobile in-app purchases
  2. Cloud-based wallets – PayPal, Amazon Pay
     - Use other authentication approaches
  3. Card network digital wallet models – Visa Checkout, Masterpass, Amex Express Checkout
  4. Guest checkout via mobile browser and app (no Card on File)

Analyzed Potential Risks and Security Gaps Across Wallet Use Case Functions

- Wallet functions

Account Creation

ID & Verification

Authentication

Integration of Mobile Device / Operating System

Use of Third Party Service Providers

- Types of attacks
  - Data breach, malware/virus
  - Account takeover fraud (ATO), new account fraud
  - Mobile device-porting fraud, man-in-the-middle/browser attack, fingerprint spoofing
  - Social engineering

1. “Pay” Wallet Security Controls – Mobile POS and In-App

- Follow EMVCo tokenization specifications and other wallet security controls
- Require consumer enrollment before token provisioned
- Issuer ID&V for mobile POS and in-app payment
  - Vets payment credentials before token provisioned to mobile phone wallet
- Payment token with dynamic cryptogram sent with transaction in lieu of PAN
  - User Authentication – fingerprint or passcode/PIN on mobile device for each POS or in-app purchase
  - Optional authentication data collected from mobile device, e.g., geolocation, device ID to identify suspicious transactions

Pay

pay

pay

Samsung Pay

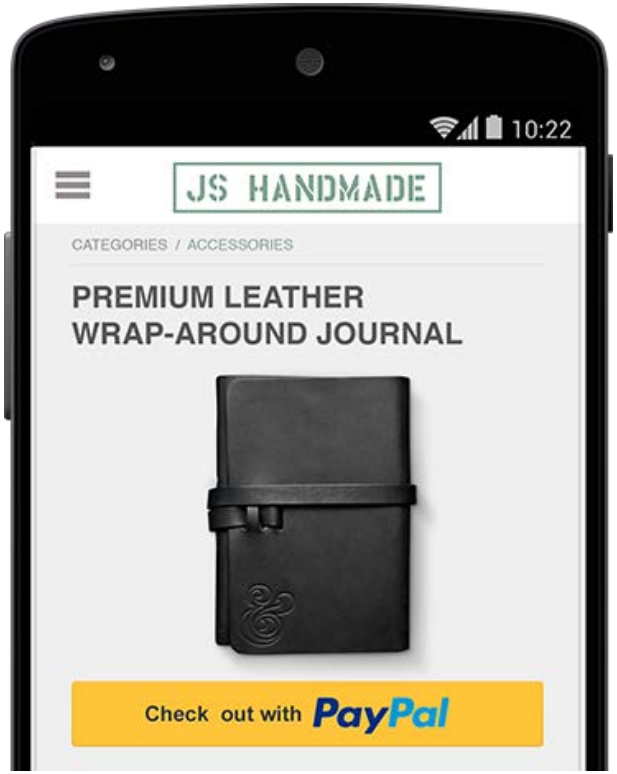
1. “Pay” Wallet Risk Assessment

- **LOW** probability of risk from fraud attacks/threats
  - Secure mobile OS/device architecture protects wallet app from malware/virus
  - Wallet app stored in protected/encrypted area of mobile phone
    - Secure Element – hardware only (Apple)
    - Host Card Emulation (HCE) – software only (Android)
    - Trusted Execution Environment (TEE) – hybrid (Samsung)
  - Tokenization prevents theft and reuse of real PAN – payment credentials not stored in phone- if transaction hacked OTA to POS or website, token useless to fraudster since can’t use token on another device or use cryptogram twice
  - Customer authentication required for each transaction prevents Account Takeover if phone lost or stolen
  - Strong issuer ID&V should identify a ‘stolen PAN’ through vetting process for provisioning to prevent New Account Fraud during enrollment
  - Apple iOS and Android operating systems prohibit access to Pay wallets if mobile phone is jail-broken or rooted

2. Payment Service Provider (PSP) Cloud-Based CoF Models

Model includes PayPal, Amazon Pay and large online merchants

- Enrollment
  - User creates account
  - Enrolls payment credentials with PSP processing on behalf of merchant, or enrolls directly with online merchant
- Authentication to PSP
  - User selects PSP from participating merchant's mobile website or app
  - Enters his PSP login credentials to complete purchase
- Authentication to merchant
  - User logs in to merchant account
  - Merchant applies payment credentials stored on file to pay for online purchase



2. PSP Cloud-based Wallet Risk Assessment

- **MEDIUM to HIGH** probability and magnitude of risk related to Account Creation
  - Account takeover fraud (ATO) is one of largest growing attack vectors
    - CNP accounts vulnerable – most common stolen data is username and password
    - Fraudster inputs username and password to access and take over multiple online customer accounts
  - PSPs and large merchants mitigate this fraud risk using sophisticated risk engines and modeling tools to analyze data
    - Perform behavioral analytics and transaction monitoring
    - Review customer profile data
    - Apply other authentication methods
    - Develop risk scores to accept or decline transactions

3. Card Network Digital Wallet CoF Model

- Merchant adds issuer/network branded button to mobile browser or mobile app checkout page
- Customer enrollment:
  - Automatically enrolled by issuing bank into wallet with existing bank credentials (network option)
  - OR creates account on digital wallet provider website
- Customer purchase:
  - Clicks button at checkout
  - Logs in to digital wallet to authenticate, authorize purchase

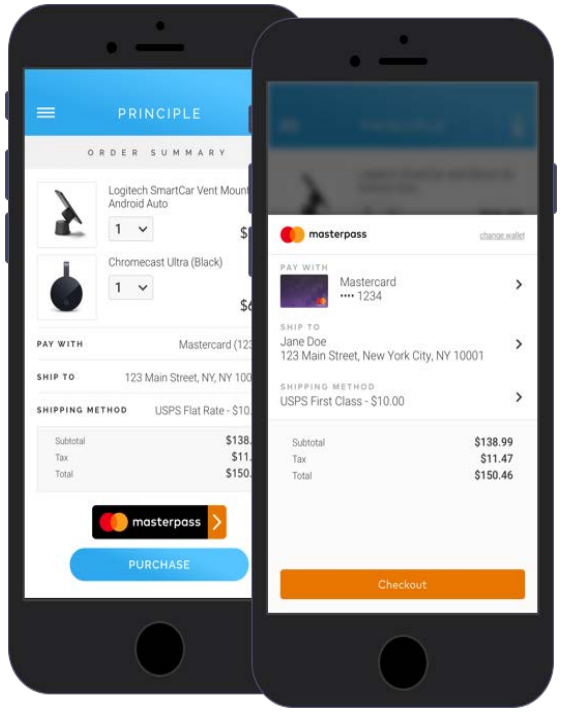
➢ **LOW** to **MEDIUM** probability of risk

- No payment credentials stored on file with merchant
- MasterCard, Visa & AmEx provision payment token to digital wallet during enrollment
- PAN not passed to merchant
- Enrolling through issuing bank further reduces risk

masterpass

AMEX EXPRESS CHECKOUT

VISA Checkout

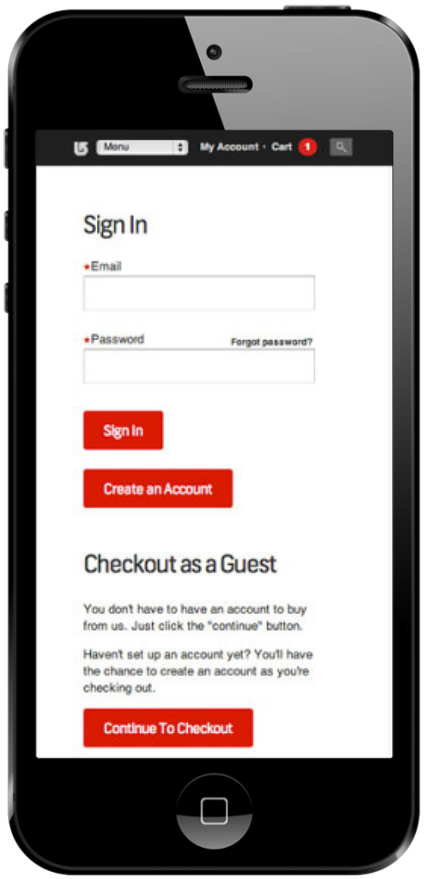


4. Guest Checkout (No Card-on-File)

- Customer access via mobile app or mobile browser
  - Manually enters PAN and PII via mobile browser/app for each purchase
- Many consumers reluctant to store PAN/PII with merchant for privacy/security reasons
- 66% of top 100 retailers offer guest checkout
  - Do not store payment credentials
  - Do not require account creation

➢ **MEDIUM** to **HIGH** probability of risk from fraud attacks/threats across all functions

- Authentication biggest merchant challenge: less information about guests
  - Merchants can effectively manage risk with proper tools and fraud detection systems



CNP Security Controls & Methods

- Tokenization (Payment and Security)
- Encryption
- Dynamic cryptograms
- Risk-based Mitigation
  - Authentication
  - Identification & Verification (ID&V)

CONSUMER SECURITY BEHAVIORS

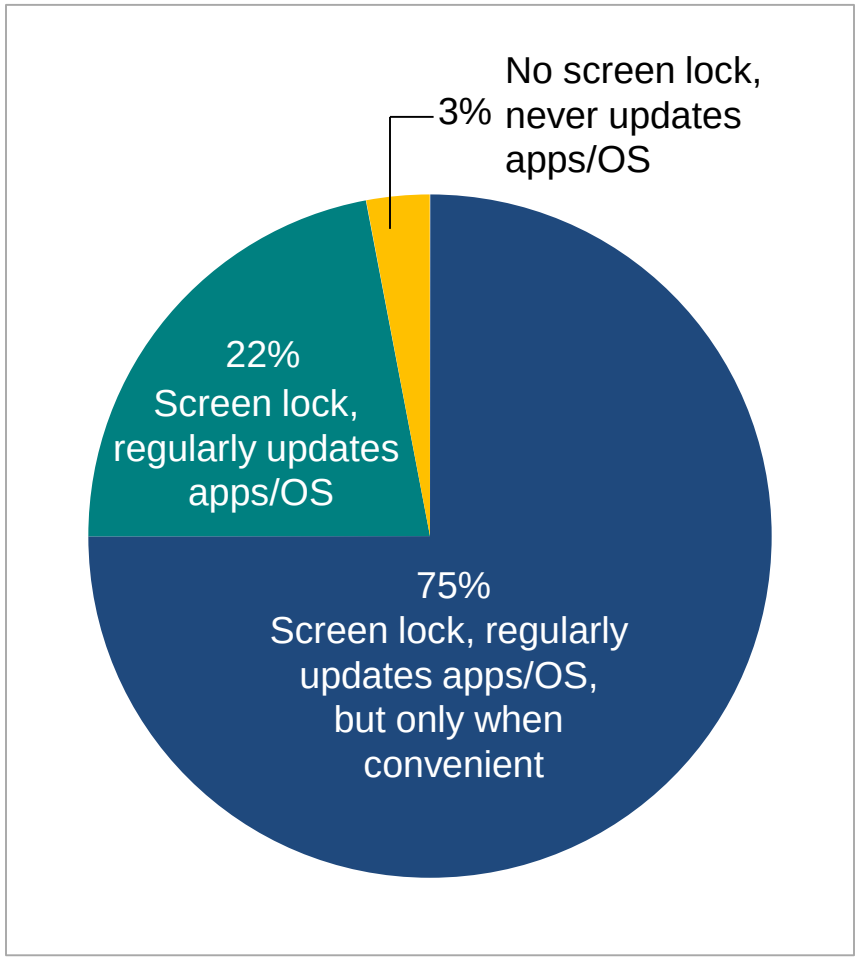
Customer Mobile Payment Adoption Barriers

- Security and fraud potential remain the primary concerns of potential users.

Source: 2016 Federal Reserve Consumers and Mobile Financial Services Report

Most Consumers Indicate They Are Taking Some Steps To Secure Their Phones

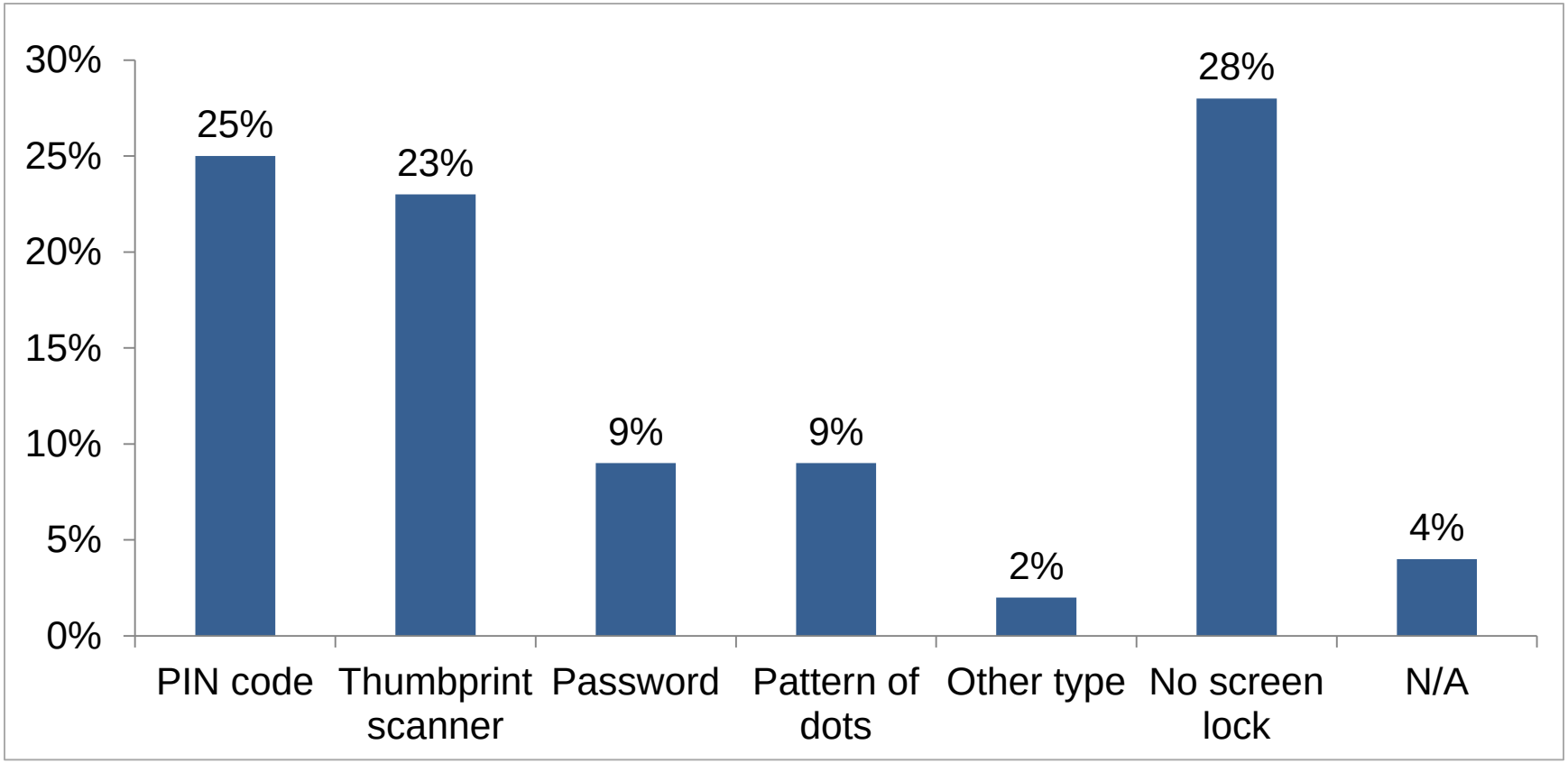
- 22% of smartphone users are diligent, take steps most recommended by cybersecurity experts
  - Use a screen lock
  - Update apps automatically or as soon as an update is available
  - Immediately update phone's OS when a new version is offered
- Most users take some security precautions
  - Use a screen lock
  - Update their phone's apps and OS when it is convenient
- Only 3% of mobile phone owners ***never*** update their mobile apps/OS or use a screen lock



Source: Pew Research Center, 2016

Consumers Use a Variety of Options to Secure Their Mobile Devices

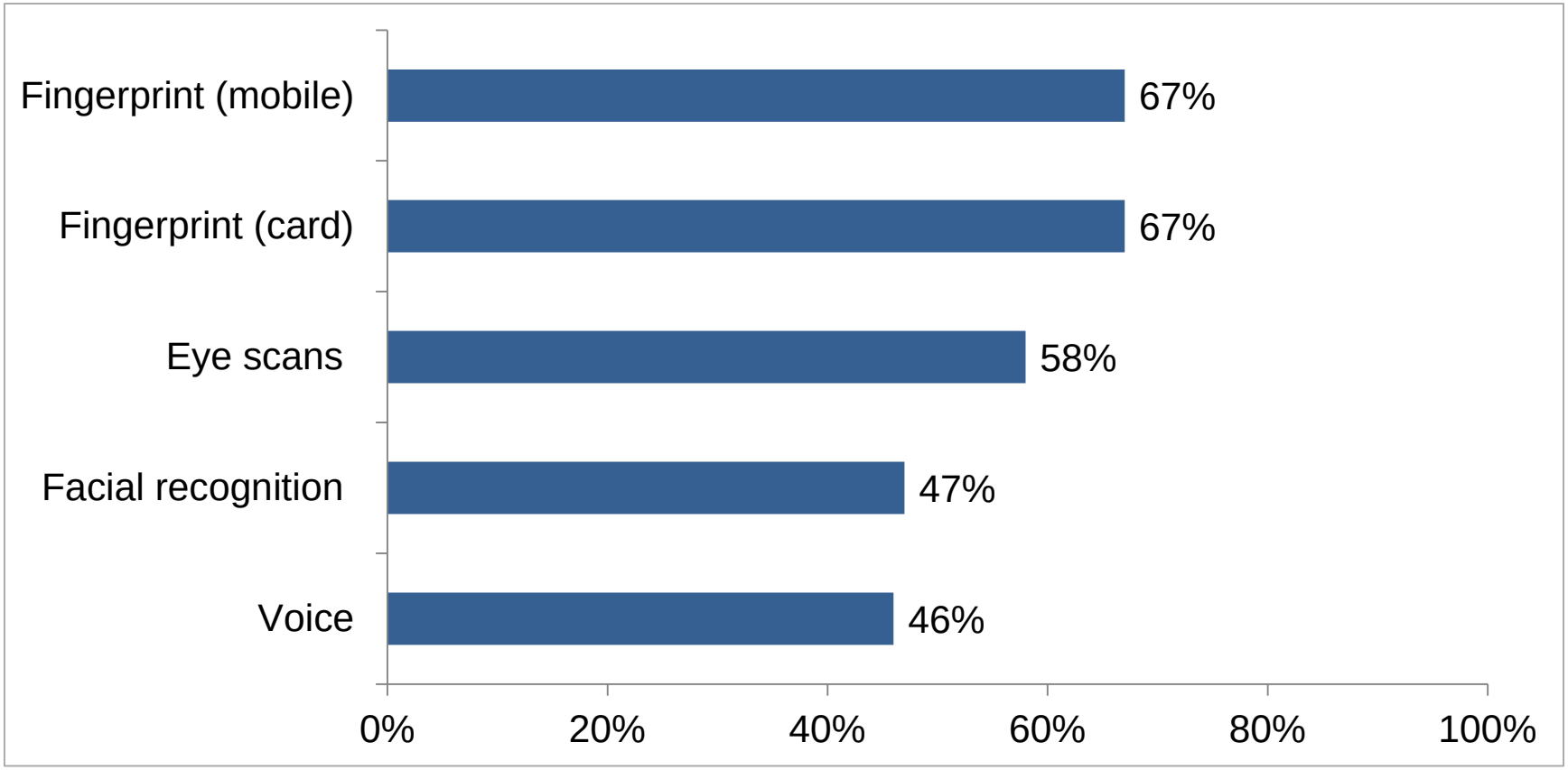
Percentage of smartphone owners who secure their device data



Source: Pew Research Center, May 2016

Consumers Warming to Biometrics

Millennial consumers surveyed expressed comfort with using a range of biometric authentication options to pay with mobile phones or cards



Source: VocaLink, 2016

Key Takeaways For Mobile Payment Stakeholders

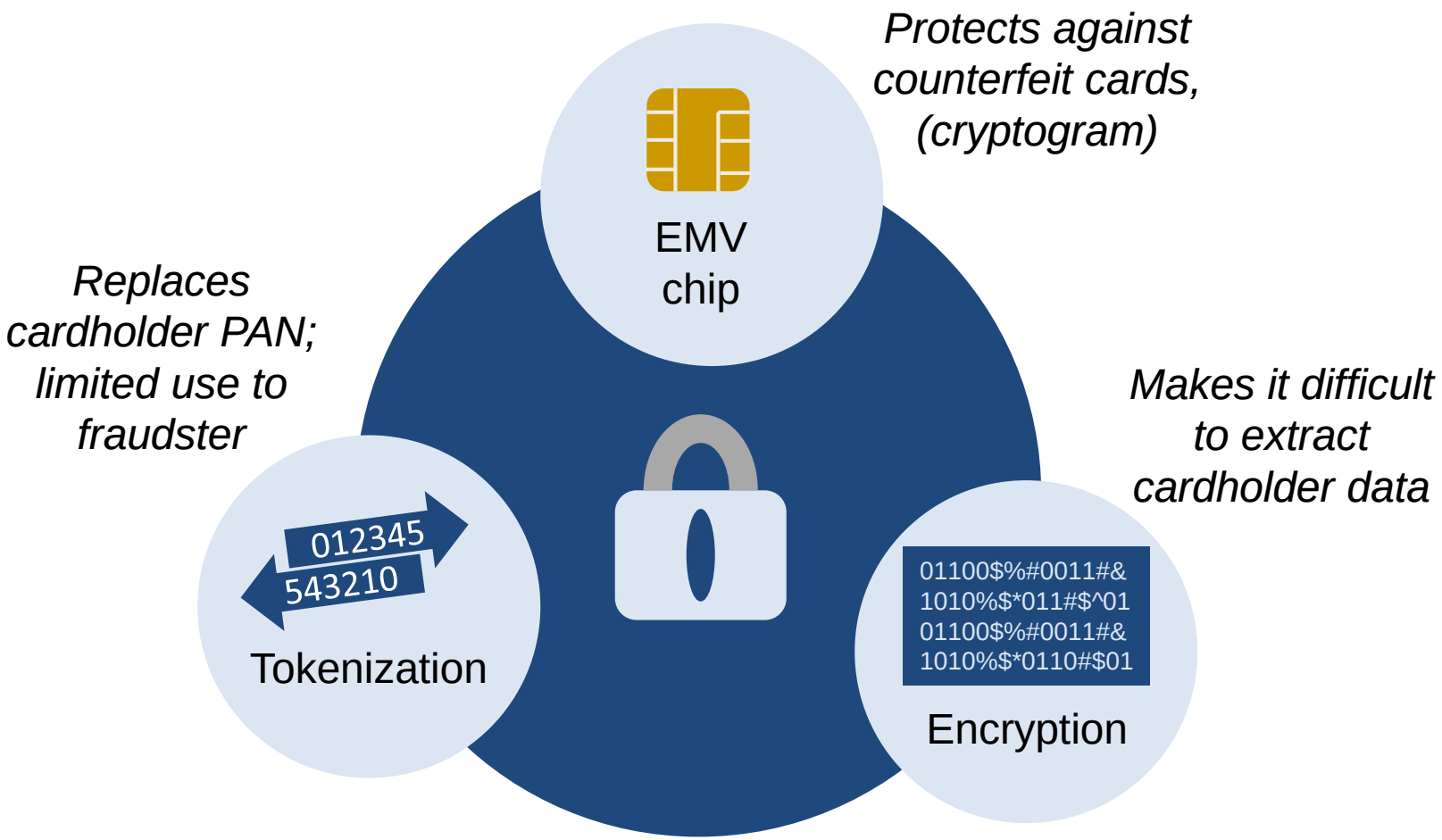
- Mobile payments can be made extremely secure with use of effective tools and monitoring
  - Develop mobile fraud management strategy but manage mobile commerce as a separate channel
  - Use multi-layered and multi-factor authentication security controls
  - Do not store actual payment account data on mobile phones or in merchant systems
    - Use payment tokens that are securely stored in mobile phone or cloud (SE, HCE O/S, TEE)
    - Use encryption to remove sensitive payment card data from transaction end-to-end and follow PCI guidelines
  - Certify third-party mobile payment apps to avoid malware/ spyware
  - Monitor third party provider access and responsibilities for your wallet solutions

Industry Collaboration On Education and Best Practices

- Consumer education on mobile payment security will help protect from hacks, phishing and identity theft
  - Do not use public WiFi networks for sensitive activities (e.g., online shopping and mobile banking)
  - Tools for physical and logical security of mobile devices
    - Know who to contact and how to remotely disable wallet if lost or stolen
    - Use strong password to protect phone and wallet
- Stakeholder education
  - For smaller merchants, particularly those in online space and their processors, to make sure they and their customers are protected
- Industry collaboration and information sharing on actions to mitigate mobile CNP fraud:
  - Fraud information sharing
  - Standards/best practices to mitigate payment fraud
  - FFIEC guidance: http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix-e-mobile-financial-services.aspx

MOBILE SECURITY BEST PRACTICES

Layered Security Approach Reduces Fraud



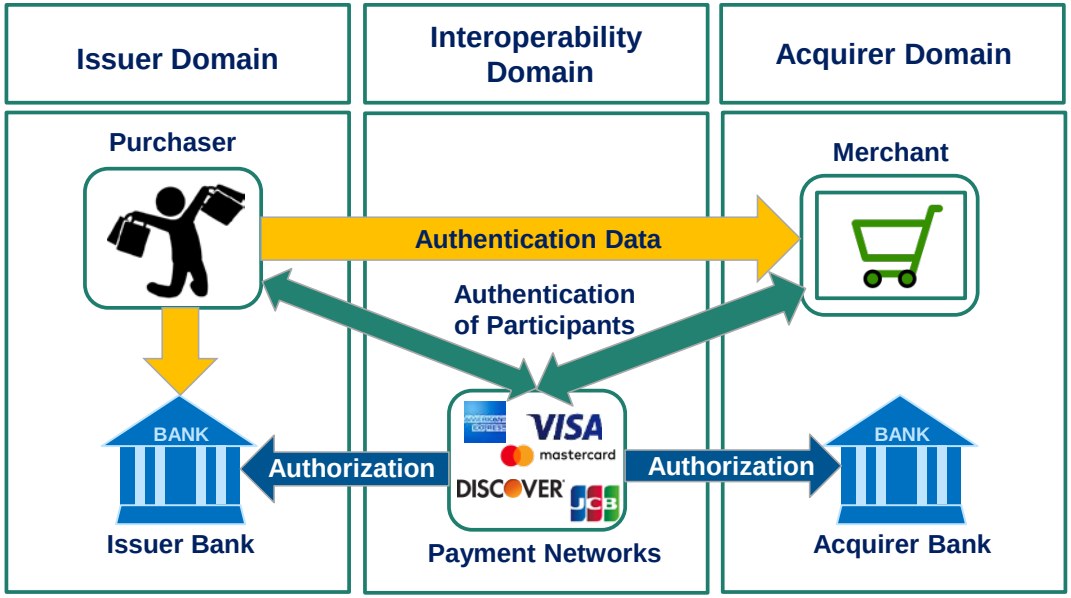
Tokenization and Encryption Protect Payment Data In-Transit and At-Rest

- Payment tokenization
  - Replaces high-value payment card account credential (PAN) with substitute value for mobile or digital financial transactions
  - EMVCo card network token spec
- Security tokenization
  - Replaces underlying sensitive value (PAN) with a non-sensitive token value post-authorization for data at-rest stored in merchant/acquirer database
  - Proprietary merchant/acquirer models
- Key Benefits of Tokenization:
  - Completely removes original payment card data from systems
  - Token value is meaningless to hackers
  - Not mathematically reversible
  - Can be formatted to maintain same structure and data type as legacy payment card data fields

Risk-based Authentication Improves eCommerce Security

- Secure communication protocol
- Enables real-time, step-up cardholder authentication directly between merchant and issuer
- Liability for fraudulent transactions shifts to issuer
- 3DS 2.0 –
  - Risk-based decisioning
  - Authenticates ONLY when risk exceeds predetermined level
  - More data elements provided to support decision
  - Additional authentication on 5 – 20% of transactions
  - Supports mobile app, mobile browser and internet/PC browser

EMVCo 3DS 2.0



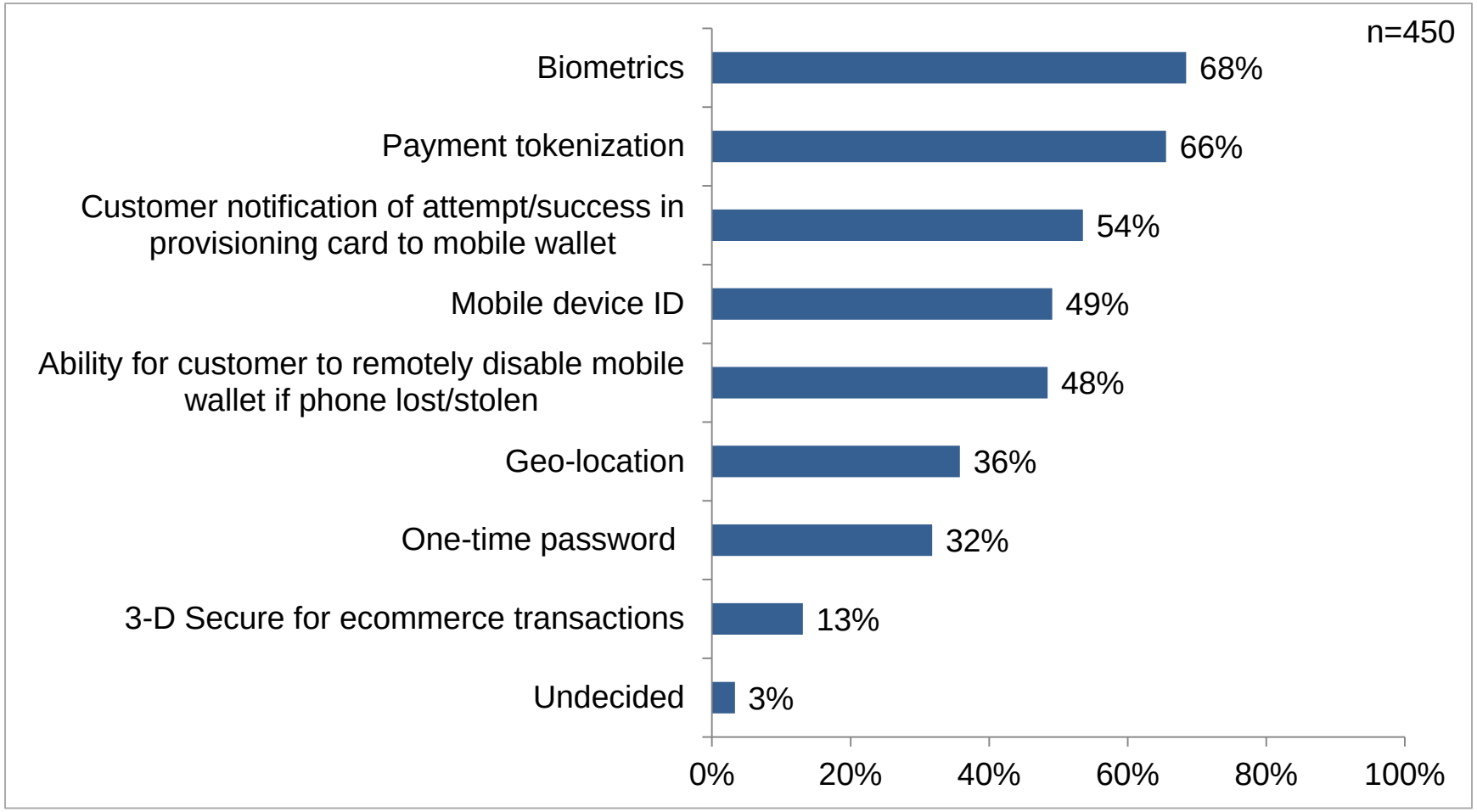
- Reduces customer friction/cart abandonment
- Improves checkout speed and convenience

Source: EMV Migration Forum, 2015

Merchants Use Multiple Security Controls

- Choice based on business, customer mix, type of mobile wallet offered, cost
- Authentication
  - Multi-factor authentication is best practice
  - Mobile device data
    - Device ID to analyze device attributes and anomalies, geolocation
  - AVS & CVV common but limited
- Real-time fraud monitoring
  - Data profiles and risk-based rules engines
- Risk-based authentication
  - 3DS 2.0

FIs Leverage Multiple Security Tools



Q47. Do you use or plan to use the following mobile security tools? (Check ALL that apply)

Source: 2016 Federal Reserve Mobile Banking and Payment Survey of Financial Institutions

Questions & Discussion

Ask a Question:
- Click the "Ask Question" button in the webinar tool
- Email rapid@stls.frb.org

For more information:
Dave Lott
David.lott@atl.frb.org
404-498-7529